



macromedia®
CONTRIBUTE™ 2

Deploying Contribute



Trademarks

Afterburner, AppletAce, Attain, Attain Enterprise Learning System, Attain Essentials, Attain Objects for Dreamweaver, Authorware, Authorware Attain, Authorware Interactive Studio, Authorware Star, Authorware Synergy, Backstage, Backstage Designer, Backstage Desktop Studio, Backstage Enterprise Studio, Backstage Internet Studio, Contribute, Design in Motion, Director, Director Multimedia Studio, Doc Around the Clock, Dreamweaver, Dreamweaver Attain, Drumbeat, Drumbeat 2000, Extreme 3D, Fireworks, Flash, Fontographer, FreeHand, FreeHand Graphics Studio, Generator, Generator Developer's Studio, Generator Dynamic Graphics Server, Knowledge Objects, Knowledge Stream, Knowledge Track, Lingo, Live Effects, Macromedia, Macromedia M Logo & Design, Macromedia Contribute, Macromedia Flash, Macromedia Xres, Macromind, Macromind Action, MAGIC, Mediamaker, Object Authoring, Power Applets, Priority Access, Roundtrip HTML, Scriptlets, SoundEdit, ShockRave, Shockmachine, Shockwave, Shockwave Remote, Shockwave Internet Studio, Showcase, Tools to Power Your Ideas, Universal Media, Virtuoso, Web Design 101, Whirlwind and Xtra are trademarks of Macromedia, Inc. and may be registered in the United States or in other jurisdictions including internationally. Other product names, logos, designs, titles, words or phrases mentioned within this publication may be trademarks, servicemarks, or tradenames of Macromedia, Inc. or other entities and may be registered in certain jurisdictions including internationally.

This guide contains links to third-party websites that are not under the control of Macromedia, and Macromedia is not responsible for the content on any linked site. If you access a third-party website mentioned in this guide, then you do so at your own risk. Macromedia provides these links only as a convenience, and the inclusion of the link does not imply that Macromedia endorses or accepts any responsibility for the content on those third-party sites.

Opera® browser Copyright © 1995-2002 Opera Software ASA and its suppliers. All rights reserved.

Apple Disclaimer

APPLE COMPUTER, INC. MAKES NO WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING THE ENCLOSED COMPUTER SOFTWARE PACKAGE, ITS MERCHANTABILITY OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY PROVIDES YOU WITH SPECIFIC LEGAL RIGHTS. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM STATE TO STATE.

Copyright © 2002-2003 Macromedia, Inc. All rights reserved. This manual may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without prior written approval of Macromedia, Inc.

Third Party Software Notices and/or Additional Terms and Conditions can be found at <http://www.macromedia.com/go/thirdparty/>.

Acknowledgments

Writing: Donald Booth, Kim Diezel

Managing Editor: Rosana Francescato

Editing: Lisa Stanziano, Anne Szabla, Mary Ferguson

Production Management: Patrice O'Neill

Print Design and Production: Adam Barnett, Christopher Basmajian, John Francis

Special thanks to Chris Bedford, Chris Denend, George Fox, Deb Galdes, Sue Hove, Joel Huff, Erik Larson, Eric Lerner, Sheila McGinn, Kimberly Oslob, Emilio Passi, Jonathan Quint, Brian Schretzmann, Ken Sundermeyer, Mitsuko Yoneyama, Contribute Beta Testers, and the Contribute engineering and QA teams.

First Edition: July 2003

Macromedia, Inc.
600 Townsend St.
San Francisco, CA 94103

Deploying Contribute to Departments and Enterprises

Macromedia Contribute is a powerful desktop tool that enables users across an organization to connect to and edit web page content. This article provides a set of best practices for deploying Contribute to multiple users within an organization. The article is intended for website administrators and IT professionals. It covers required network and server permission settings and the role of Contribute permission groups. It also provides tips for defining appropriate Contribute connection paths.

In addition, this article gives suggestions for setting up Contribute to meet the needs of various website structures, from sites as simple as a root folder with multiple user-specific folders to multiple group folders with specific access groups.

Finally, this article describes some strategies for using Cascading Style Sheets (CSS) and Macromedia Dreamweaver templates in a site and for using Dreamweaver and Contribute collaboratively to edit web pages.

Administrator's Checklist for Deploying Contribute

Use the checklist below to guide you through the key tasks of setting up Contribute users to edit existing websites. The checklist also includes tips for using Dreamweaver and Contribute together on websites.

- 1 Create an administrator connection to the website using the Contribute Connection Wizard (Windows) or Connection Assistant (Macintosh).
- 2 Set up network and web server permissions to allow read/write/modify access as needed so that users can update the website files.
- 3 Determine the Contribute site administration requirements appropriate for your website.
- 4 Define Contribute permission groups as needed based on the controls you want to place on a user's ability to edit pages on the site.
- 5 Distribute Contribute to your users.
- 6 Send connection keys to your users so that they can access their website files and folders.
- 7 Create CSS and Dreamweaver templates so that Contribute users can use the product more effectively and you can maintain control of the site's layout and style elements.
- 8 Configure settings for Dreamweaver users so that they can work safely with Contribute sites.

Step 1: Create an administrator connection

Website administrators manage Contribute websites by controlling who has access to the site and by specifying the types of edits content creators can make in a website.

You use the Contribute Connection Wizard (**Edit > My Connections > New**) to create a new website connection. To become a website administrator, in the Administrator Information screen of the Connection Wizard select **Yes, make me the administrator**. If you are becoming the administrator of an already established site connection, choose **Edit > Administer Websites**; then select **Yes** when prompted.

About matching network paths and web address (URLs)

When creating a connection to the website, Contribute prompts you to provide the web address (URL) of the website, and the network or the File Transfer Protocol (FTP) information of the server and folder storing the website. Both the web address and network path must point to the same folder in the website.

For example, if your website is located at the directory path \\MyServer\wwwroot\sites\MySite, and the corresponding web address for this site is www.myserver.com/sites/MySite, then you must correctly enter these values in the Contribute Connection Wizard (Windows) or Connection Assistant (Macintosh) when creating the connection.

To ensure the website and network folder (or in the case of FTP, the FTP folder) are the same, Contribute uploads a temporary file using the path information you provide. Contribute then attempts to read the temporary file via HTTP using the web address you provided. If Contribute succeeds in locating the temporary file, the paths match and Contribute creates the connection. If the paths don't match, Contribute prompts you again for the correct path.

If your users will use FTP to connect to a website folder beneath the FTP Host folder, you must provide an absolute folder path to the folder.

Use Contribute with a local network

When Contribute is used to connect to a web server through a local network, the web server must be visible to the local network. Contribute can also be used with VPN servers to ensure that all file transmissions occur behind your firewall. If the web server is not visible to the local network, you can create an FTP connection with Contribute to work with the website.

To ensure that you are entering the correct network path, use the Browse button of the Connection Wizard to locate and select the network folder. If the path to the folder is correct, but Contribute is still unable to create a connection, verify that the folder has proper read/write permissions.

To learn how to check your server's network and folder permissions, refer to the documentation supplied with your server operating system.

Use Contribute with FTP

As you create an FTP connection with Contribute, Contribute attempts to auto-detect the FTP path, checking that the FTP folder is the same folder that contains your website files. If the folder paths don't match, Contribute can't write to the page displayed by your browser and prompts you to enter the correct path.

To ensure that you are entering the correct FTP path, use the Browse button of the Connection Wizard to locate and select the FTP folder. If the path to the folder is correct but Contribute still can't create a connection, verify that the folder has proper read/write permissions for the user. If you are creating an anonymous FTP account, the server must be configured to support delete, rename, and overwrite permissions for the anonymous user. In some cases, file permissions on UNIX servers may be configured in a way that prevents Contribute from operating, especially if the server doubles as a file server. For more information, see "Setting up a site connection in Contribute" on the Macromedia Contribute Support Center.

Step 2: Set Up Network and Web Server Permissions

Contribute users in your organization access the web pages they edit either through a local area network connection or by using FTP. To ensure that their connections work and that they can edit the pages, check that they have the correct network and server administration permissions to connect to and modify pages in the website folders.

You cannot set network administration and server permissions using Contribute. These tasks are completed using the standard network administration management tools.

The network and file server permissions you set determine whether users can access another computer over the network, read or open files or folders, and delete or modify files. Before sending a connection key to content editors in your organization, you should check that network and file server permissions are set correctly so that users can read, write, and modify pages they need to update.

For example, if the files the user will update are on a server named *HRAAdmin*, in a folder named *HRSite*, you must make sure they are able to access *HRAAdmin* and have read, write, and modify permissions to the *HRSite* folder.

Additionally, Contribute users must have proper administrative permissions to update files on their local machines: the ability to read, write, and modify files locally. When Contribute users publish a page to the web server, a copy of the page is stored locally on their computer. A Contribute editor that can't update files locally is not able to edit the pages.

Set folder permissions

In addition to setting network permissions, you also need to ensure that folder permissions are properly configured to allow users to modify files. For example, in Windows, to set user permissions for a network folder, you use the Properties dialog box. You right-click the folder you want to set properties for, and then select Properties. In the Security tab, set the permissions to allow or deny access to folders as appropriate.

Note: You can set folder permissions to allow a user or group of users to modify a folder and later define more restrictive folder- or file-editing options when you set Contribute permission group options.

If the Contribute users will use FTP to access the web server, make sure that the website folder has delete, overwrite, and rename privileges enabled. When using anonymous FTP, these file-protection options are typically disabled by default. This prevents users from connecting to the website, publishing updates to pages, and adding new pages to the website.

To test that FTP is set up correctly for an end user, you can transfer a test web page to the server. Then, using the login settings you will provide to the user, attempt to view the page in a browser.

Whenever you provide access to a web server, you should take proper security measures to ensure that both the operating system of the server hosting the site and the web server software itself (and the FTP server, if using FTP) are secure. For the best practices for securing your website from both accidental and malicious tampering, see the documentation provided with your server's operating system, FTP, and web server software.

Disable browsing of Contribute generated folders

When you create a site connection, Contribute creates special files that are stored in folders whose names begin with an underscore (such as `_mm`, `_baks`, and `_notes`). These folders may contain files with user names, e-mail addresses, and previous versions of the web pages. The underscore allows Dreamweaver and Contribute to distinguish between those folders and the other folders in your site.

Contribute and Dreamweaver use this naming convention to filter these special files and prevent them from being displayed in the Dreamweaver Site panel and in the Contribute Remote File Browser. These hidden folders can't be browsed, overwritten, or inadvertently altered by users. Additionally, most search engines and automated programs are designed not to return pages found in folders whose names begin with an underscore.

Apache web servers

If your website uses Apache, you can explicitly disable the browsing of folders and files that begin with an underscore. If you know how to modify the Apache web server's `httpd.conf` file and have permission to do so, you can use the `DirectoryMatch` directive to prevent visitors from viewing any file in a folder beginning with an underscore.

If you're not sure how to edit the Apache `httpd.conf` file or don't have permission to do so, ask your system administrator or Internet service provider (ISP) to do it for you. To learn more about limiting access to files and folders, and other security issues relevant to the Apache web server, see the documentation supplied with your Apache distribution.

Microsoft IIS web servers

Microsoft IIS does not provide high-level filtering of specific folders in the same way that Apache does. To achieve some level of filtering, you can use the file system's hidden flag to hide individual folders from general access. This will cause IIS to return a 404 File Not Found page for a URL pointing to the specific underscore folder. If you want to filter the folders, you have to set the hidden flag individually for each folder you wish to hide. If directory listings are not enabled for the folder, this setting isn't necessary, since without directory listings users automatically get a 403 forbidden error when browsing to a folder path web address.

Note: It is very important that this hidden flag be set for folders only and not the files inside them. Hiding files contained in an underscore folder may cause Contribute and Dreamweaver to stop functioning correctly.

Any user who is aware of the naming convention for underscore folders and files could still type in the specific folder and filename, and then, in some cases, view the files in the browser. However, using the hidden flag on these folders reduces the likelihood of this happening.

Other web servers

If you are using another vendor's web server, refer to the documentation supplied with the software to learn how to prevent users from accessing specific folders and files.

Step 3: Determine Site Administration Requirements

Before you create the administrator site connection, you should determine, based on the website's structure and the needs of Contribute users, where to create the website connection. As the administrator, you can establish a connection to the root folder in a website to access all the folders in a website or establish a connection to a lower level folder, depending on the access you need.

Contribute does not allow you to create overlapped (or nested) connection paths. For this reason, you should create a connection to the highest required access level in the site structure. If you need to limit users to folders below this level, you can use Contribute Permissions settings to specify specific folder access and editing options. For information about setting up permission groups, see [“Step 4: Define Permission Groups”](#).

Here is an example of overlapped site connection paths:

Paths overlapped

connection1: <http://www.mysite.com/intranet/>

connection2: <http://www.mysite.com/intranet/marketing>

Paths not overlapped:

connection1: <http://www.mysite.com/intranet/marketing>

connection2: <http://www.mysite.com/intranet/finance>

Shared settings

Contribute creates a special folder (_mm) containing a shared settings file (contribute.xml) in each website to which you create a connection. The shared settings file contains information about each permission group you define, including the administrator permission group. If you are creating multiple site connections for different sets of users, make sure the connection paths you define do not overlap. As the administrator, you should create your connection at the highest level of pertinent access to the website; you can define user permission groups to allow users access at lower levels of the site depending on their specific access requirements.

The shared settings can be altered only by entering the site administrator's password. You should store the shared settings on the website server so that you can easily update the user permissions when necessary. By controlling the site from the server, you will not need to resend a connection key. The changes are automatically applied when the user connects to the site.

Permission groups

With Contribute, you can set sitewide settings, which apply to all users with access to a site, as well as permission group settings, which apply to user groups you define. A permission group is a set of permissions that define which folders users can access and make edits to, as well as what kinds of edits they can make. For example, you can allow or deny users the ability to create or delete pages, specify whether they use font tags or inline style, and define the pages or templates on which they base new pages.

You can define any number of Contribute permission groups and specify different options for different permission groups. Contribute permission groups are not based on system or network user groups. You can send the same connection key to members of different workgroups. As long as the recipients have appropriate access to the network or server folder, they can edit the website. Because Contribute permissions are not tracked, there is no record of which users are using a particular permission group.

You should create user group names according to your users' needs. These names simplify the task of managing the permissions assigned to a particular group. For example, if one group will have access to the Sales site and full editing permissions, and another group will have text-only editing permissions, you might name the first group Sales-Full, and the second Sales-Text, and so on.

Define shared setting and permission requirements

Now that you know how shared settings work and how an administrator can set up specific permission groups to limit user access, you can consider some different scenarios for setting up Contribute for large or multiteam organizations.

This section describes three primary configurations for Contribute administrators to consider as they determine how to set up Contribute sites.

Keep in mind that the main issues in successfully setting up multiple users are: (1) defining where the shared settings file is stored, (2) preventing connection paths from overlapping, and (3) sending customized connection files to each group of users. Depending on how your website is structured, you need to use different strategies for setting up access for various groups of users.

Use the information in this section to help you determine where to create the shared settings file for the following common website structures:

Flat website centrally administered Typically, this is a website where users have read access to the root of the site and read/write access to specific folders in the site as controlled by the file server or network permissions. There is a single root folder, and all users are part of the same Contribute permission group. If this applies to your site, see [“Deploy Contribute for a flat website structure using file system controls”](#).

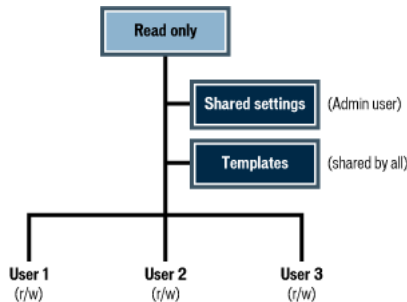
Deep website centrally administered In this structure there is a single root folder. The root folder contains folders for each section or organizational function within the website. Contribute permission groups are used to control user access to particular folders on the site, and to assign a subset of the common templates used in the site. Although not required, file server permissions are usually used in addition to Contribute permission groups to restrict user access to sections of a site. If this applies to your site, see [“Deploy Contribute to a deep website structure”](#).

Deep website with distributed administration In this structure, separate groups take responsibility for specific sections of a website. Access may be further divided so that users in a particular group have permission to edit only specific folders in their section of the site. Sites of this type may have multiple administrators. This is effectively like setting up each department or group with a separate Contribute-enabled website, and each site will not share common files such as templates. If this applies to your site, see [“Deploy Contribute to sites consisting of multiple separate websites”](#).

Deploy Contribute for a flat website structure using file system controls

This structure is useful for creating faculty or employee home pages, a series of collaborative team websites, small business websites, and departmental websites that have independent web servers and web administrators. The key to this arrangement is that all users have the same set of Contribute permissions. In other words, there is a single permission group in the shared settings file that controls the behavior of Contribute when editing the website. There also may be a single set of Dreamweaver templates (if the site uses Dreamweaver templates) shared by all users. For such sites, the administrator defines and restricts different users to different parts of the site using file system permissions.

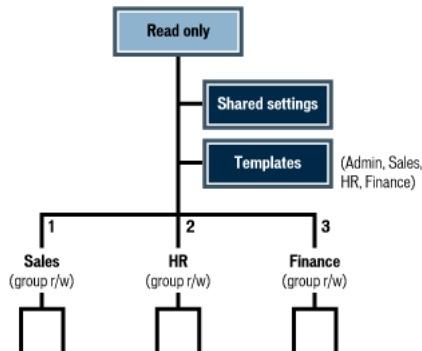
In addition to storing shared settings and templates, you can store CSS style sheets, Server Side Includes (SSIs), images, and other sitewide “read-only” assets off the site root.



In this scenario, the administrator uses the Connection Wizard (Windows) or Connection Assistant (Macintosh) to create a site connection to the root folder (for example, /myIntranet). In the Administer Websites dialog box (Edit > Administer Websites), the administrator defines a Permission group that gives all users access to the folders in /myIntranet. Any user connecting to the site with this connection key has access to all the folders in this directory.

Deploy Contribute to a deep website structure

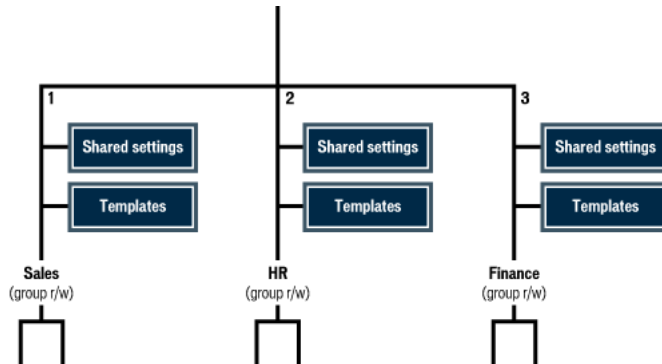
The following structure works best with larger, centrally controlled websites, such as corporate intranets, public government websites, or university websites. In this structure there is typically a single administrator who uses site templates, and possibly department templates, to control the central site. The separate site sections are maintained by different contributors. The site administrator sets up a single shared settings file for the entire site and then defines a permission group for each section of the site. Each Contribute permission group is restricted to the appropriate section of a site and is given access to the subset of templates used in its section of the site. At the file server level, individual users are given read access to all sections of the site; and read, write, and modify access to the section of the site they are allowed to edit.



In this scenario, the administrator creates a site connection to the root folder (for example, /myIntranet). In the Administer Websites dialog box (**Edit > Administer Websites**), the administrator creates three permission groups for users and sets user access to a specific folder. For example, for a Sales site Contribute user, the administrator selects the Folder/File Access option, and then allows only members of this user group to edit content in the folder at /myIntranet/Sales.

Deploy Contribute to sites consisting of multiple separate websites

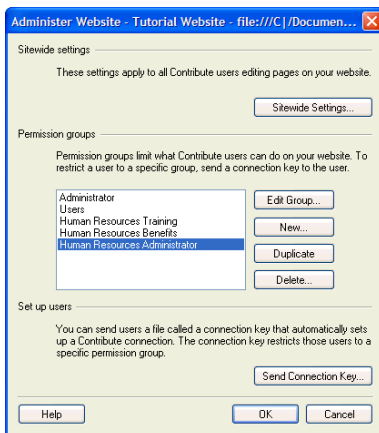
In the following scenario, there are multiple administrators for the site, one for each section. Each administrator can set up a site for Contribute users. The templates for each section of the site are kept in template subfolders for each section. As in the previous example, the other users can browse the full site but are restricted to editing only their folder. This provides a different level of flexibility while keeping Contribute files out of the root of the site. This structure also allows each group to act more independently.



In this scenario, three administrator connections are created. The site administrators create a connection to their department's section of the website (for example, /myIntranet/Finance). Additional Permission groups can be created to define any restrictions for users in the site (for example, to specific subfolders in the Finance folder or to set editing options).

Step 4: Define Permission Groups

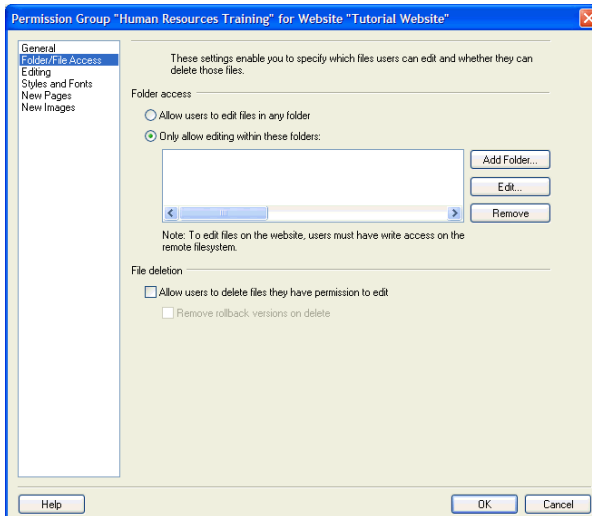
After you determine your site administration requirements, setting up Contribute permission groups is a very straightforward process. You use the Administer Websites dialog box (**Edit > Administer Websites**) to create permission groups and define sitewide settings as needed.



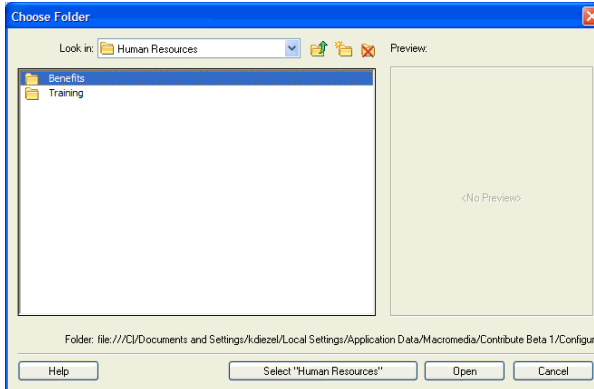
Tip: It is best to limit your sites to no more than 25 permission groups. In some cases you may encounter performance problems if you create more than 50 permission groups.

To restrict a permission group to access specific folders:

- 1 In the **Permissions Group** list select the permission group you are setting permissions for, then click **Edit Group**.
- 2 In the Edit Group dialog box, select **Folder/Files Access** and select **Only allow editing in these folders**.



- 3 Click the **Add Folders** button, then choose the folder in the website that members of this permission group can edit.



In this example, content creators who receive this permission group will be able to make edits to any folders in the Human Resources folder.

For additional information about Permission group settings, see Managing User Settings and Permissions in Contribute Help (Help > Macromedia Contribute Help) and Macromedia TechNote 16611, “Options for Contribute website administrators”.

Step 5: Distribute Contribute to content editors

Contribute is a desktop program. Each Contribute user must install and use it on their local machine. Most administrators who deploy Contribute to multiple users already have a system in place for deploying desktop programs in their organizations. Remember that restricted users may not be able to install programs and that some folders and files may be off limits. For this reason, a desktop administrator may need to install Contribute for such users.

You can post Contribute on an intranet site or local network for download. You can also distribute Contribute on a CD. In all cases, you must accept and comply with the terms and conditions of the volume licensing agreement.

Step 6: Send Users a Connection Key

To set up Contribute users, you need to provide them with the basic site connection information for the web server. This is done by sending them a connection key.

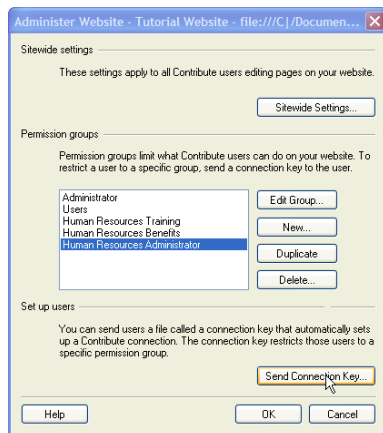
Connection Keys

A connection key is a file generated by Contribute that contains all the information that Contribute requires to connect to a site. The information in the connection key is encrypted with a 128-bit algorithm for security purposes. End users cannot read or change the connection or permission group information in the connection key. Administrators create these password-protected connection keys using the Send Connection Key feature of the Administer Websites dialog box. The keys can be sent to end users by e-mail, or saved to the network.

Connection keys do not automatically expire. To invalidate a connection key, you must delete the permission group from the shared settings files. You do this in Contribute through the Administer Websites dialog box (**Edit > Administer Websites**). If a user uses a connection key that refers to a deleted group, the message box alerts the user to contact the site administrator.

Send a connection key

The easiest way to get end users connected is to send them a connection key by e-mail. You can use the **Send Connection Key** option in the Administer Websites dialog box.



When you use this option Contribute automatically launches the default e-mail application and generates an e-mail with a connection key attachment and simple instructions to help the user get started. As the administrator, you must send end users the connection key password information they need to access the website. Typically, you send the password information in a separate e-mail message or contact the users by phone.

After receiving a connection key, a Contribute user simply double-clicks it to start the connection process. The file is encrypted, so the user must know the password that the administrator defined for the key. Connection keys also specify what permission group settings to apply. When the correct password is supplied, Contribute automatically makes a connection to the site and allows page edits as defined for the associated permission group.

Step 7: Use CSS Style Sheets and Dreamweaver Templates

You can use Cascading Style Sheets (CSS) and Dreamweaver templates to control the look and feel and the layout of pages in your sites, maintaining sitewide consistency.

Cascading Style Sheets help you ensure consistent text formatting and allow you to define additional styles for Contribute users to apply in the pages they edit. Dreamweaver templates let you define the areas of a page a Contribute user can edit.

By using templates, you can lock regions of a page that you do not want a user to edit. You can use the full range of Dreamweaver template options in a Contribute site. For example, you can create templates that include optional regions, repeating regions, template properties, and so on. You can also use nested templates to design department- or site-specific page layouts that are based on other templates. For additional strategies for preparing sites for Contribute users, see *Optimizing Web Development for Contribute Users: A Strategy Guide for Site Administrators*.

Cascading Style Sheets (CSS)

You cannot use Contribute to attach a Cascading Style Sheet to a page, but you can edit a page with a style sheet already attached. Use Dreamweaver to define CSS styles for an individual document or to create a style sheet that you can attach to multiple documents. Contribute recognizes CSS styles attached to a page and allows the user to use these styles. Contribute users can use the Styles pop-up menu to apply styles that have been defined in the page or in an attached style sheet.

Tip: You can make it easier for Contribute users to work with CSS styles: Name the styles so that they make sense to Contribute users. For example, you can provide a more descriptive name like MainHeading, Title, or Headline instead of Heading, depending on how your user is likely to use the style.

Each style you define in the attached style sheet appears in the Styles pop-up menu. If you want to keep certain styles from appearing in the menu, add “mmhide” before the style name (for example, mmhideNavTable).

For more information about using CSS, see these resources on the Macromedia website:

- Using Cascading Style Sheets in Contribute
- Best Practices with CSS in Dreamweaver MX

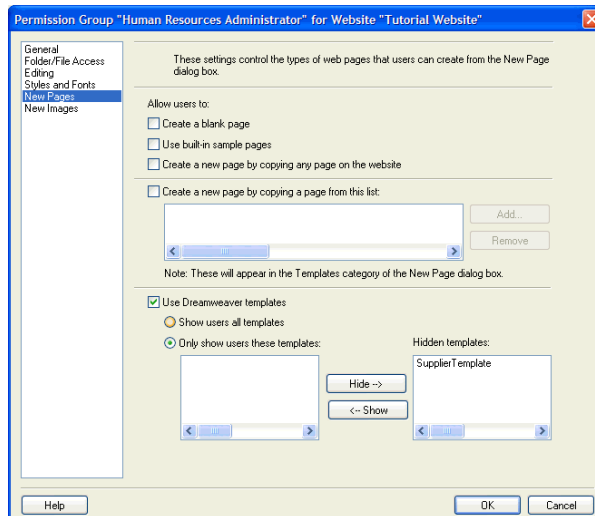
Dreamweaver Templates

Dreamweaver templates are powerful design tools that help a website administrator or developer control which areas of a page a content contributor can update. Dreamweaver templates are made up of editable and noneditable regions. Content contributors can make edits only in predefined editable regions of the page. By using Dreamweaver templates, you can reuse design and layout elements and maintain consistency across multiple website pages. You can use the Administer Websites dialog box to define which templates a particular permission group has access to.

To be used in a Contribute site, the Dreamweaver template files, identified by the .dwt file extension, must reside in a folder named Templates in the root folder of the website (for example, */Templates/contactPage.dwt*). When you create templates in Dreamweaver, they are automatically saved in a Templates folder, but you will need to publish the folder to the web server. If users do not have access to the root folder or are restricted to a subfolder in the website, you need to copy the Templates folder to the appropriate site subfolder to provide access to the templates.

To limit a permission group to specific templates:

- 1 In the Administer Websites dialog box, select the Permission group you want to set up templates for, then click **Edit Group**.
- 2 In the Permission Group dialog box, select **New Pages**.
- 3 Deselect the options in the **Allow users to** section, if you want to disable those options.
- 4 To specify which templates to use, do one of the following:
 - If the permission group can use all templates in the site, select **Show users all templates**, then click **OK**.
 - Select **Only show users these templates**, then in the **Hidden templates** list select the templates you want to make available. Click the **Show** button, and then click **OK**.



Step 8: Configure Dreamweaver MX Settings

When using Dreamweaver MX and Contribute together, the site administrator needs to make sure Dreamweaver MX Design Notes are enabled and are uploaded to the web server.

Dreamweaver MX users should install the Dreamweaver MX 6.1 Updater to take advantage of the new site options available for integrating with Contribute. This also ensures that features like Check In/Check Out and Rollback work seamlessly between Dreamweaver MX and Contribute users.

Users of older versions of Dreamweaver should ensure that Check In/Check Out are enabled and that Design Notes are always uploaded to the web server. These options are part of the site settings. All Dreamweaver users should ensure that any existing pages they are editing have been properly checked out to prevent inadvertent overwriting of pages. They should ensure that their sites are connected to the same site root folder as the Contribute users.

Summary

Understanding how Contribute interacts with the server is important for a smooth implementation of the program in a large organization. Understanding the server permissions requirements not only ensures that Contribute is working smoothly but also reassures webmasters that the site is secure and stable, allowing them to keep an eye on the big picture. Allowing Contribute users to update their own content enables everyone to work more efficiently. A good understanding of the Contribute workflow ensures that updates, synchronizing, and sitewide changes can be implemented smoothly. Properly implemented, Contribute allows users to easily update their content and reduces the hassle for webmasters.